REMARKS

Applicant respectfully requests reconsideration of the present application in view of the reasons that follow.

Discussion of Rejections under 35 U.S.C. § 103:

In the outstanding Office Action dated March 9, 2011, claims 1, 5-7, 9, 10, and 12 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over U.S. Patent Publication No. 20040203783 to Wu et al. (hereinafter "Wu"), U.S. Patent Publication No. 2002/0174335 to Zhang (hereinafter "Zhang"), and further in view of U.S. Patent No. 6,178,244 to Takeda et al. (hereinafter "Takeda"). Further, claims 2, 8 and 11 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Wu, Zhang, Takeda, and further in view of U.S. Patent Publication No. 20030009691 to Lyons et al. (hereinafter "Lyons"). Applicant respectfully traverses these rejections for at least the reasons that follow.

As discussed in Applicant's previously filed responses, independent claims 1, 7, and 10 of the present application at least require that an application is enforced to switch any traffic provided over internet access to the UT (in the public WLAN) to an encrypting security service port. That is, after an ACP initiates the AAA procedure for a UT and after the UT is authenticated at the AAA back-end system, the ACP forces applications to switch traffic to an encrypting security service port when the UT tries to access the Internet IP (i.e., any traffic provided over internet access).

In rejecting independent claims 1, 7, and 10 of the present application, the Examiner asserted that "Wu teaches enforcing an application to switch any traffic provided over internet access to the user terminal in the public wireless local area network to an encrypting security service port (paragraphs 12, 30, 31, 39-40, and throughout the reference, where handoff keys are used and users are transferred to different access points" (emphasis added). See, page 3 of the outstanding Office Action. Applicant disagrees. Wu is explicitly clear in describing that the use of handoff keys and encryption in that context is limited to communications between a terminal and AP during a handoff (e.g., a handoff authentication message). See, figures 3, 4; paragraphs 30, 31, 39-41 of Wu. Thus, Wu fails to teach or

suggest that "any traffic provided over internet access to the user terminal" is switched to an encrypting security service port. Again and to be clear, various embodiments of the present application are directed to encrypting those communications/traffic (resulting from applications) between a UT and, e.g., the Internet, that occur after the UT has already been authenticated/authorized with the AP.

Additionally, the Examiner correctly recognized that the alleged combination of Wu and Zhang fail to teach "wherein traffic is switched to an encrypting security service port upon determining that the access to the public wireless local area network is not encrypted" (emphasis added). However, the Examiner asserted that column 27, lines 17-30 of Takeda cure this deficiency of Wu and Zhang. Applicant disagrees.

Column 27, lines 17-30 of Takeda recite the following:

> The router 141 is connected to the WAN and Ethernet switches 131 and 132 are connected to the router 141. The ciphertext port of the encryptor 501 for connecting to the LAN is connected to one of the ports of the Ethernet switch 131. The plaintext port of the encryptor 501 is connected to a general HUB 121. The ciphertext port and the plaintext port of the encryptor 502 are connected in the same way. Plaintext data received by the general HUB 121 or 122 is input to the plaintext port of the encryptor 501 or 502, is encrypted and output to the Ethernet switch 131 or 132 from the ciphertext port. The data flows in ciphertext through the WAN, the Ethernet switch 131 or 132 and the router 141, that is, the output direction side of the ciphertext port of the encryptor 501 or 502.

Nowhere in this section of Takeda, nor anywhere else in Takeda for that matter, is there any teaching or suggestion of a determination that access to a public wireless local area network is not encrypted, let alone switching internet access traffic to an encrypting service port upon such a determination. This section of Takeda merely describes how ciphering/encryption is achieved in a particular system.

To the above, it appears that the Examiner has merely found a reference, Takeda, which describes an encryption procedure, and alleged that because the prior art teaches encryption, it would be obvious to "determine" that traffic is not encrypted, and then encrypt

it. Applicant disagrees. Again, and as described at, e.g., page 1, line 13-page 2, line 20 of the present application, conventional public WLANs do not encrypt internet IP communications, and have no known key distribution mechanisms. To overcome the shortcomings of the prior art without the need for new software/hardware, various embodiments of the present invention enforce encryption through traffic switching to an encrypting security service port when it is determined that internet access is unencrypted.

Moreover, and even if the teachings of Takeda were to be combined with Wu and Zhang, the system still would not result in the claimed features of the present invention. That is, the purpose of Takeda is understood as providing a cryptosystem, where logical groups can be formed, wherein the encrypting is done via a session key. For example, Takeda describes the following at column 6, lines 12-39:

> A cryptosystem according to the present invention includes:
>
> a plurality of groups of communication terminals;
>
> a plurality of encryptors, each of which corresponds to at least one of communication terminals, and each of which comprises:
>
> (a) a session key memorizing unit for memorizing at least one session key for encrypting/decrypting communication data sent/received by the communication terminal which belongs to each of the plurality of groups;
>
> (b) a cipher processing unit for encrypting/decrypting the communication data using the session key; and
>
> (c) a data sending/receiving unit for sending/receiving the communication data processed by the cipher processing unit.
>
> According to the invention, a cryptosystem includes a plurality of cipher managing domains, each of which includes one of a plurality of key managers, at least one encryptor and at least one communication terminal. In the cryptosystem, each of the plurality of key managers includes a session key generating unit for generating a session key to be used for its own cipher managing domain. And in the cryptosystem, one of the session key generating unit of the plurality of key managers generates a common session key for the other key managers to be used for

> ciphertext communication among the plurality of cipher managing domains. (emphasis added).

Thus, and at best, the combination of Wu, Zhang, and Takeda, would merely result in a system that encrypts the communications between an AP and terminal in Wu (that utilizes a session key) according to the cryptosystem methods taught by Takeda. However, this combination still would not achieve any feature analogous to/suggestive of at least "upon determining that the access to the public wireless local area network is not encrypted, enforcing an application to switch any traffic provided over internet access to the user terminal in the public wireless local area network to an encrypting security service port." (emphasis added).

The cited references fail to teach or suggest at least the above-discussed feature of the pending claims. Neither Zhang nor Lyons nor Takeda cures this deficiency of Wu. Therefore, the cited references, either alone or in combination, fail to teach or suggest each feature of the pending claims.

Therefore, the pending claims are not *prima facie* obvious in view of the prior art. Accordingly, independent claims 1, 7 and 10 are patentable. Further, claims 2, 5, 6, 8, 9, 11 and 12 each depend from one of allowable claims 1, 7 or 10 and are, therefore, patentable for at least that reason, as well as for additional patentable features when those claims are considered as a whole.

Conclusion:

Applicant believes that the present application is now in condition for allowance. Favorable reconsideration of the application as amended is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 50-5302. Should no proper payment be enclosed herewith, as by the credit card payment instructions in EFS-Web being incorrect or absent, resulting in a rejected

or incorrect credit card transaction, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 50-5302. If any extensions of time are needed for timely acceptance of papers submitted herewith, Applicant hereby petitions for such extension under 37 C.F.R. §1.136 and authorizes payment of any such extensions fees to Deposit Account No. 50-5302.

Respectfully submitted,

Date June 9, 2011

By /Sanjeev K. Dhand/

ALBERTDHAND LLP
Customer Number: 12268
Telephone: (858) 764-2453
Facsimile: (858) 430-4886

Sanjeev K. Dhand
Registration No. 51,182
Attorney for Applicant